# Security As A Service Framework For Broadband Users University Of Nairobi

ROTICH ERICK KIPTANUI, ROBERT OBOKO

**Abstract**: Currently most businesses rely on broadband to run networks and web applications. This means introduction of vulnerabilities in Universal Resource Locator (URL) that are in connection. Effective monitoring of URLs is crucial for any organization; each port has vulnerabilities associated with it. This research project explored the use of Security as a Service (SaaS) business model to deliver security to users through a web based technology. The project implements a web based technology software with an aim to assist broadband users to scan for vulnerabilities in a URL based on open ports or ports in use and suggest ways of mitigating the vulnerabilities discovered. Results from several sample websites are given, exceptions, constraints and achievements. The project also compares the findings to related previous work and then gives a conclusion and recommendation for further work.

**Index Terms—** SaaS, Application service provider (ASP), Internet Assigned Numbers Authority (IANA), Uniform Resource Locator (URL)

---

## I. INTRODUCTION

### A. Background

Computer data and applications security is a fundamental aspect of computing that if taken care of can improve users computing experience. To safeguard users from malicious attacks and disruptions, most computers are protected using PC based anti-virus or anti-malware applications and personal firewalls. These measures though are effective in normal computer environments, are no longer effective for businesses that have embraced the broadband and fiber optic connectivity. The emergence of broadband and fiber optic connectivity provides opportunities for users to improve their work environment while at the same time opens the users to wide range of data and network security threats. The threats are a result of fiber optic connectivity design that provides their users with at least one public static or dynamic Internet Protocol IPs. Most users are aware of the situation while others are not. Those that are aware of their public IP still have no way of ensuring their applications, data, and network components are safe.

### B. Definitions and Concepts

***a)*** **Vulnerability scanning**

Vulnerability scanning is similar to packet sniffing, port scanning [28]. Vulnerability scanning is the automated process of proactively identifying vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened. While public servers are important for communication and data transfer over the Internet, they open the door to potential security breaches by threat agents, such as malicious hackers. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, Testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security. Vulnerability scanning typically refers to the scanning of systems that are connected to the Internet. Itt can also refer to system audits on internal networks that are not connected to the Internet in order to assess the threat of rogue software or malicious employees in an enterprise.

**2) Port scanning**

Port scanning is the Sending of queries to servers on the Internet in order to obtain information about their services and level of security. On Internet hosts (TCP/IP hosts), there are standard port numbers for each type of service. Port scanning is also widely used to find out if a network can be compromised. A port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed for weakness [29].

**3) Web application scanning**

Web application scanning is a method used to test web applications for common security problems such as cross-site scripting, Sequel Language (SQL) injection, directory traversal, insecure configurations, and remote command execution vulnerabilities. Scanning tools crawl a web application and locate application layer vulnerabilities and weaknesses, either by manipulating Hypertext Transfer Protocol HTTP messages or by inspecting them for suspicious attributes [31].

**4) Network scanning**

Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweep and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer. Another scanning method, inverse mapping returns information about what IP addresses do not map to live hosts; this enables an attacker to make assumptions about viable addresses [30].

**5) Software as a Service (SaaS)**

Software as a Service - also known as SaaS, is new business concept that has potential to revolutionize the way people have used software traditionally. A Software as a Service (SaaS) model - is hosted generally on centralized network servers to make functionality available over web or Intranet. From developer point of view [19], such SaaS can be managed and maintained easily compared to hassles involved in other software models. For end users such service is easy to consume and there is a possibility of using such service on pay per use basis

.

## II. PROBLEM STATEMENT

Currently most businesses rely on broadband to run network and web applications. This means introduction of vulnerabilities through open ports at any instance in URLs that are in connection. Each open port has vulnerabilities associated with it, hence the dilemma of which ports are Open? What are the vulnerabilities to these open ports? How can these vulnerabilities be mitigated?

### A. Significance of the study

This research project will be of great significance given the current state of vulnerabilities facing the broadband users. The main significance of this study are outlined below.

#### *a)* Network vulnerability discovery and Suggested mitigation

Network perimeter vulnerabilities will be discovered and mitigation measures suggested. Security alerts can be provided for specific flows thus raising the level of awareness.

#### *b)* Improved security manageability

Through special dashboards users will have an informative look of their security status. The visualization tools will help users to address the most important areas of their security.

#### *c)* Enhance broadband and fiber optic adoption .

The high level of security awareness will facilitate higher adoption rates for broadband. Users will be comfortable with connectivity since their data and a dedicated provider will monitor application security

.

#### *d)* Maximize Return on Investment for security services

Since software as a service is a model that involves metered usage from a reliable provider, users will only pay for what they use as opposed to current means of software procurement. The security providers have expertise in the area and are therefore able to give services at cheaper rates.

## III. OBJECTIVES

From the problem statement of this research, our focus will be to achieve the following key objectives:

**a)** To study software as a service framework.
**b)** To create agents to perform port scan to find open ports.
**c)** To show vulnerabilities associated with the open ports
**d)** To suggest possible mitigation.

### A. Figures

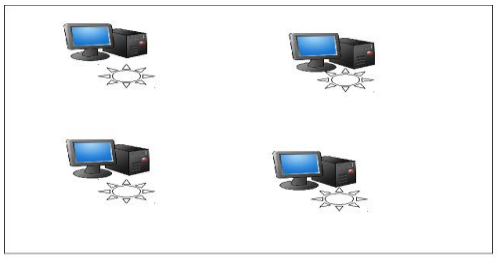

**Fig: 1** classical security setup; with anti-virus/anti-malware software on each workstation

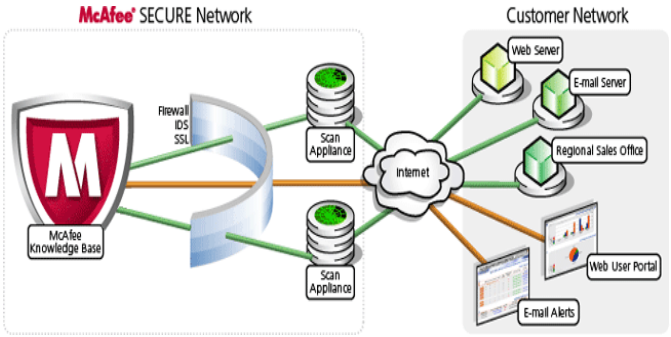


**FIG 2:** MCAFEE SECURITY-AS-A-SERVICE

## IV. LITERATURE REVIEW

### A. Review of literature and related work

#### *a)* F-Secure

Have signed an agreement to offer protection for PCs to all customers using 3 Italia's Internet dongles to access the web [8]. 3 Italia's Internet security solution which is provided by F-Secure, is a full security suite which, in addition to antivirus, includes several other functionalities such as Browsing Protection, Firewall, Antispam and Parental Control which cares for the safety of children when they access the web.

#### *b)* BinarySEC© SaaS

BinarySEC© SaaS is an example of security as a service solution which blocks all abnormal traffic on a company's website before it reaches its server and protects against data theft, deny of service, identity theft and new attacks from the web [8].

#### *c)* McAfee Security-as-a-Service

McAfee Security-as-a-Service solutions are designed to provide organizations of all sizes, from small to large enterprises, with a comprehensive set of security products built on a Software-as-a-Service model. This strategy leverages McAfee's core strength in threat prevention. [16]

#### *d)* Port Numbers

A port is an interface on a computer to which you can connect a device and a port number is part of the addressing information used to identify the senders and receivers of messages. The port numbers are divided into three ranges

i. The Well-Known Ports are those from 0 through 1023.
ii. The Registered Ports are those from 1024 through 49151.
iii. The Dynamic and/or Private Ports are those from 49152 through 65535

#### *e)* Well Known Port Numbers

The Well-Known Ports are assigned by the Internet Assigned Numbers Authority (IANA) and on most systems can only be used by system (or root) processes or by programs executed by privileged users. Ports are used in the TCP to name the ends of logical connections, which carry long term conversations. For the purpose of providing services to unknown callers, a service contact port is defined. This list specifies the port used by the server process as its contact port. The contact port is sometimes called the "well-known

port"..The range for well-known ports managed by the IANA is 0-1023[15].

***f)*** Webroot® E-Mail Security SaaS

Webroot® E-Mail Security SaaS delivers enterprise-class security with better manageability, better value and better protection than any other e-mail security solution. There is no hardware or software to deploy meaning a lower total cost of ownership and guaranteed protection against Spam, viruses and service downtime [32].

***g)*** **Online protection and email storage from McAfee and Reboot Twice**

The power of online security protection and email storage solutions is at your fingertips. With convenient online ordering, you can put SaaS security solutions to work for your business [19]. Zscaler provides risk mitigation and policy enforcement for businesses through its cloud service, while enriching the user's Internet experience. Organizations do not need to purchase, deploy, or manage countless point products. Companies simply define their corporate security control and compliance policy by accessing the Zscaler utility. The web traffic leaving the network firewall is easily redirected to data centers in Zscaler's global infrastructure. Based on an organization's policy, traffic is blocked, throttled, or allowed to access the Internet. As the browser retrieves the web pages, Zscaler scans it for a range of malware threats and delivers clean traffic to the end user [21].

***h)*** **Cloud Provisioning - SaaS Framework**

The Cordys Business Operations Platform (BOP) is web-based and fully SaaS (Software-as-a-Service) enabled, with no client implementation requirements other than a web browser. The Cordys SaaS Deployment Framework enables companies to mix and match legacy software with services available in the Cloud or to launch new web-based services to customers [10].

***i)*** **Dynamic cloud provisioning**

The SaaS framework creates new application usage patterns, in which users may add applications and services on the fly, new SaaS consumers (tenants) may join or leave on a daily basis and customers are billed per usage. To address the requirements of these usage scenarios, Cordys provides the SaaS Deployment Framework (SDF) which enables dynamic cloud provisioning of applications and rapid on-boarding of tenants. M anages the relationships between applications, tenants and users; and measures (meters) utilization of billable entities [10].

### B. SaaS Deployment Models

***a)*** **Pure SaaS application**

i. Web browser is single interface point with customer
ii. All intelligence is centralized at SaaS provider
iii. Limited integration between customer and SaaS provider
iv. Examples: CRM, Email filtering, Payroll, Customer support applications

***b)*** **SaaS with customer side software agent**

i. Web browser is interface point with customer
ii. Additional small client-side software agent (permanent or transient)
iii. Enables stronger integration of customer systems and SaaS service
iv. Examples: Application sharing, Web-filtering, Online-Backup

***c)*** SaaS with customer side appliance

The Web browser is interface point with customer the additional hardware appliances are remotely managed on customer premise. This enables deep integration of customer systems with SaaS providers, i.e. Intrusion Detection, Security Management and Vulnerability Assessment

### C. Nsauditor network security auditor

Nsauditor Network Security Auditor is a network security scanner that allows auditing and monitoring network computers for possible vulnerabilities, checks your network for all potential methods that a hacker might use to attack it. Nsauditor is a complete networking utilities package that includes more than 45 network tools for network auditing, scanning, monitoring and more [17].

### D. Advanced Port Scanner

Advanced Port Scanner is a small, fast, robust and easy-to-use port scanner for Win32 platform. It uses a multithread technique, so on fast machines you can scan ports very fast. Also, it contains descriptions for common ports, and can perform scans on predefined port ranges [18].

## V. METHODOLOGY

### A. Introduction

The research was set up to explore ways of scanning for open ports and discovers vulnerabilities and suggested mitigation.

### B. Context of the research

The conceptualized setup of the model consists of small business/startup company local area network with several web applications running on TCP/IP servers such as email server, company web site, enterprise/business applications, database servers, e-commerce applications. The LAN is opened to public users on the Internet through the router with firewall setup to filter each application that can be accessed. The business systems are exposed to good users who intend to carry out normal business activities. The systems are also exposed to malicious users and applications whose intention is to disrupt normal usage of business service. On the same front with normal and malicious user or applications, we have scan agents that can be launched to scan the URLs to discover open ports, applications and vulnerabilities facing them.

### C. Research setup

To be able to address the objectives, a system was designed with the following key features.

a) Port scanning
b) Display of general URL scan results
c) Mapping of open ports to possible vulnerability and suggestion of mitigation.
d) Display of vulnerabilities and Suggestion of mitigation to the users.

A user interface was designed to make it easy for the user to obtain and understand the results because of user friendly presentation.

### D. How the research was conducted

Before the actual port scanning commenced, a hypothetical application server/web server was set up. Then, a broadband router and firewall were configured. In using the system, the user is required to follow the following steps:

a) Open the interface.
b) Type the URL of the site being scanned for open ports.
c) Enter the port range for scanning.
d) Start scan.
e) Monitor the progress of the scan using the progress bar.
f) Display the results by clicking on view scan results button.

### E. Data collection

Data collection was mainly done through scanning the ports of a given domain. The user provides the URL of the domain during the initialization of scanning.

The system was subjected to the following types of websites:

i. E-commerce
ii. Educational web sites

From the scans, the data collected included:

a) Open ports.
b) Closed ports.
c) MySql specific scans.

### F. Data analysis

The port number was used to determine whether a site is vulnerable or not. The vulnerability of website or domain depends on

a) Port Number.
b) Type of vulnerability associated with the open port.

## VI. ANALYSIS, DESIGN AND IMPLEMENTATION

### A. Introduction

This chapter outlines the Analysis, Design and Implementation of Port scanning. The chapter deals with preparations for actual implementation of the components. The discussion begins by analyzing the scanning environment that scans for open ports and asses the vulnerabilities associated with the open ports and suggested mitigation.

### B. Scanning environment analysis

#### *a)* MySQLTest agent

Mysql scan agent scans Mysql database to find out whether:

i. It uses Mysql default password (root –root) -This makes it easy for hacker to gain access to the database to view Mysql database contents and possibly copy, delete or change its contents.
ii. No Password in Mysql database - Meaning the entry is free.
iii. Password is empty – an attempt to protect the database was initiated but no password was entered.

#### *b)* Portscann agent

**The Portscann** agent pick port numbers in the range provided by the user and sends them one at a time to another agent (Scanjob). The scan job agent determines whether the port is open at the time of scan or not. If the port is open, the port number is written to the ports table and its status is flagged **yes**. Likewise if the port is closed or not in use its port number is written to ports table and its status is flagged **no**.

#### *c)* Features on the interface

**The scan user interface** is used to capture the scan parameters on the interface.

a) URL textbox – to enter the URL or Domain to be scanned.
b) Start and stop textboxes – to specify start and stop port range to perform a scan on.
c) Scan button – use to initiate the scan.
d) Close button – use to exit the interface.
e) Progress bar – Indicates that the scan is in progress.
f) View Scanned Results button – after the scan completes the uses this button to display results.
g) Ports not in use pane – Displays the port numbers that are not in use.
h) Ports in use pane – Displays the port numbers that are in use.
i) General URL test pane – Displays the URL specific vulnerability checks.
j) Vulnerability and suggested Mitigation pane – Displays vulnerabilities associated with the open ports and suggested mitigation.
k) Textarea to display the port numbers ranges as shown below.
   i. The Well-Known Ports are those from 0 through 1023.
   ii. The Registered Ports are those from 1024 through 49151.
   iii. The Dynamic and/or Private Ports are those from 49152 through 65535.

The user can enter short ranges or long ones depending on what ports they are interested in. a port range can be specified as follows

| Start | Stop |
|---|---|
| 0 | 500 |
| 500 | 3000 |
| 0 | 65535 |
| 49151 | 65535 |
| 80 | 80 |

**Table 1. Port number range examples**

### C. Deployment

This application will be deployed using the SaaS with customer side software agent model where desktop client is interface point with customer and additional small client-side software agent (permanent or transient) this enables stronger integration of customer systems and SaaS service. The deployment model will be achieved by the personalized packing of the java desktop client as an executable jar files that can be launched on any operating system platform. To achieve this, the host computer will require java run time environment pre-installed and Internet connectivity to access the public IP

### D. Summary

The design of the Scanning environment was eased by the availability of the open source platform (Java). The main challenge when using scan agent is the availability of the network connectivity . Identifying and suggesting mitigation was successful since if a port was discovered open it was

then mapped to vulnerability table to retrieve the vulnerability and suggested mitigation associated with port open.

## VII. EXPERIMENTAL RESULTS

### A. Introduction

In this chapter, illustration of how the scanning model to achieve the key functions of discovery in the port scanning and Mitigation are suggested. The scan results are generated based on whether the port is open or not. The following were the results obtained when various URLs were subjected to the system. Port number range 0-2000

### B. General results

The extent to which the port is deemed vulnerable depends on whether it is open or not, and the vulnerability strength.

***a)*** **Site A**

When Site A was subjected to the system one port number (53) was discovered to be open and the following vulnerability and the system suggested mitigation is shown in table 2 below

| Port open | Vulnerability | Mitigation |
|---|---|---|
| 53 | This could open the way for a Trojan to port 53 to bypass the firewall. | Define DNS server explicitly in the firewall configuration. |

**TABLE 2. SCANNING STATUS OF Site A**

From the above results Site A at the time of scan had only one open port, which indicated that the URL was safe.

***b)*** **Site B**

When Site B was subjected to the system four ports (110,143,21,53) were discovered to be open and the following vulnerabilities and the system suggested mitigation are shown in table 3 below.

| | | |
|---|---|---|
| 110 | Remote users can gain privileged (root) access to systems running vulnerable versions of POP servers | If you determine that your POP server is vulnerable disable the POP server. |
| 143 | When this port is opened and exposed to the outside world can create serious vulnerabilities for the users PC. | If you cannot close this port, then use a NAT router or personal firewall. |
| 21 | An attacker could connect to port 21 and instead of sending expected data, one could send something unexpected. | web-hosting websites, allow its customers to upload there files to manage there website. Its not really un-secure to be port 21 open, |
| 53 | This could open the way for a Trojan that uses port 53 to bypass the firewall | Define DNS server explicitly in the firewall configuration |

**Table 3. Scanning Status of SITE B**

Scanning results for Site B at that instance indicated that there were more open ports and hence the URL was vulnerable to threats.

***c)*** **Site C**

When Site C was subjected to the system eight ports (110,143,53,993,995,443,465,1081) were discovered to be open and the following vulnerabilities and the system suggested mitigation (some of which were not in the table at the time of run) are shown in table 4 below.

| | | |
|---|---|---|
| 53 | This could open the way for a Trojan that uses port 53 to bypass the firewall | Define DNS server explicitly in the firewall configuration |
| 110 | Remote users can gain privileged (root) access to systems running vulnerable versions of POP servers. No specific description of vulnerability | If you determine that your POP server is vulnerable disable the POP server |
| 143 | When this port is opened and exposed to the outside world can create serious vulnerabilities for the user's PC. | If you cannot close this port, then use a NAT router or personal firewall |
| 993,995, 443, 465,1081 | As per time of scan the vulnerabilities and suggested mitigation had not been put into our database | No suggestion |

**Table 4. Scanning Status SITE C**

Scan results for Site C at that instance indicated that there were more open ports and therefore the URL was more vulnerable.

### C. Malicious Users

The best way to protect yourself is to find the open ports before an attacker finds them hence address the issue of potential malicious users who can scan your URLs for open ports and launch attacks.

## VIII. DISCUSSION

***a)*** **The main findings and observations**

The results from simulations done with the scanning model developed during the research process in the previous chapter lead to the following main findings and observations

***b)*** **Scanning URL was successful.**

The model successfully achieved URL-request scanning and required services discovery. The ports could be scanned and the status determined as open or closed which are then written to a port table for further processing. Every time a scan is performed a new port table is created as long as a correct URL and start and stop port numbers are provided. The scan was successful when the URL provided was in connection and port ranges for scanning were provided. The scan fails if the URL is not in connection or the URL is using a proxy server.

***c)*** **View scanned results**

There are four panes to display scan results. The scan results were available only when there was a successful scan as discussed in (a) above. Table 3 above shows what is displayed in each pane. If no port is found open then the ports opened pane and vulnerability and mitigation panes are blank. A successful scan would always display results in pane 3 because the tests here are specific to HTTP and Mysql hence don't defend on open ports.

***d)*** **Exceptions**

The scanning process cannot be successful if the URL is not in connection. From the research it can be concluded that if the connection uses a proxy then the scan is a challenge.

***e)*** **Achievements**

The work demonstrates that it is possible to scan for open and closed ports in a given URL that is in connection. Once the scan process is complete it is possible to generate a list of vulnerabilities associated with the open ports and suggest mitigation. This research project has been developed using open source software and, a software as a service it can be used for free. The users need to download the product and follow some steps to install it in their computers.

***f)*** **Constraints**

The test environment requires that machine used in carrying out the experiment be in a constant connection to the Internet. There is need to acquire a dedicated leased line or unlimited wireless broadband connections. Some users may have problems in downloading and running the product meaning that a user intending to use this product must have some knowledge in using an operating system..

## IX. CONCLUSIONS AND FUTURE WORK

### A. The conclusion

In section 1.4 of the research work, the key objectives were shown. The main aspects of the system developed and tested were to scan ports associated with a URL and establish their status. Based on the scanned port it was then possible to tell what vulnerabilities were associated with the URL's open port(s) and then suggest Mitigation to the discovered vulnerabilities.

### B. Recommendations and Future Work

This research has focused on the scanning of URLs to establish which ports are open. The scanning and display of possible vulnerabilities in this research depend wholly on manual input, which forms a building block for future automated input. The recommendation for future work would be to develop agents to automatically generate input to built databases as subscription, list vulnerabilities and suggest mitigation. Further research on effects/impacts of related ports on security can be conducted. There is need also to explore how ports that are required to be open for the users to perform certain activities are given attention in relation to vulnerabilities that are associated with them.

## X. APPENDIX

### A. APPNDIX B – SIMPLE SCAN AGENT INSTALLATION GUIDE

a) Connect the machine to an internet connection that does not use a proxy server.
b) Copy the entire folder "ScanAgent" from the CD provided into a folder of your choice.
c) Open the folder and double click on run.bat batch file in the folder.
d) Enter the URL, start and stop port number range and start scan.
e) When the scan progress bar stops click on view scanned results button.

## XI. ACKNOWLEDGMENT

Special thanks go to my able supervisor Mr Robert Oboko for his continued assistance during this study. I also want to register my sincere gratitude to the Vlir UOS for the kind assistance they extended to my study by providing funds that gave me a big boost in doing my research. I am indebted to my family, my loving wife and children for their tireless support during this study. Last but not least thanks to my fellow students whom their continued encouragement made this study a success.

## XII. REFERENCES

1. Birth of Broadband. ITU. http://www.itu.int/osg/spu/publications/birthofbroadband/faq.html. Retrieved July 21, 2009.

2. Chong and Carraro, 2006.

3. http://eval.symantec.com/mktginfo/enterprise/white_papers/bsymc_cyber_threat_analysis_program_WP_250478.en-us.pdf

4. http://metadata.library.cornell.edu/

5. http://ntrg.cs.tcd.ie/undergrad/4ba2/presentation/

6. http://supplychaintechnology.wordpress.com

7. http://www.asl-webroot.co.uk/

8. http://www.binarysec.com

9. http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns171/ns625/ns647/net_brochure0900aecd80400060.html

10. http://www.cordys.com/cordyscms_com/cloud_provisioning.php

11. http://www.free-press-release.com/news-techcello-recently-launched-ver-2-0-of-cellosaas-1290517154.html

12. http://www.f-secure.com

13. Fyodor http://www.insecure.org/nmap
14. http://www.harborobjects.com/AllenBerezovsky/post/2009/09/24/Business-Logic-in-Stored-Procedures-or-Business-Layer.aspx

15. http://www.iana.org/assignments/port-numbers

16. https://www.mcafee.com

17. www.nsauditor.com

18. http://www.radmin.com/products/utilities/portscanner.php

19. http://www.reboottwice.com

20. http://www.software.co.il/application-security/26-practical-threat-analysis-of-complex-systems.html

21. http://www.zscaler.com

22. OECD Broadband Report Questioned. Website Optimization. http://www.websiteoptimization.com/bw/0705/. Retrieved June 6, 2009.

23. OECD Broadband Statistics to December 2006. http://www.fcc.gov/cgb/broadband.html. Retrieved June 6, 2009.

24. Sixth Broadband Deployment Report. FCC. http://www.fcc.gov/Daily_Releases/Daily_Business/2010/db0720/FCC-10-129A1.pdf. Retrieved July 23, 2010

25. (http://www.t1shopper.com/tools/port-scan/)

26. Traudt, Erin; Amy Konary (June 2005). "2005 Software as a Service Taxonomy and Research Guide". IDC. pp. 7.

27. Wainewright, Phil (October 2007). "Workstream prefers virtualization to multi-tenancy". http://blogs.zdnet.com/SAAS/?p=400. Retrieved 2008-05-24

28. http://www.webopedia.com/TERM/V/vulnerability_scanning.html

29. http://netsecurity.about.com/cs/hackertools/a/aa121303.htm

30. http://searchmidmarketsecurity.techtarget.com/definition/network-scanning

31. Elizabeth Fong and Vadim Okun Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8970 {efong,vadim.okun}@nist.gov

32. (http://www.asl-webroot.co.uk/)